ABSTRACT

A hybrid method for a service provider to transmit decryption information (e.g., algorithms, parameters, keys) to clients in a secure manner and at low cost for use in decrypting broadcast services. The service provider uses a bi-directional channel (e.g., a GPRS channel) to receive service requests, authenticate clients and transmit currently valid decryption information (and, optionally, future decryption information) necessary to decrypt a broadcast service. The service provider transmits the encrypted service on a unidirectional channel (e.g., a DVB-T channel). The service provider preferably also changes the encryption of the service with time, and, as it does, transmits updated decryption information to its clients on the unidirectional channel. The updated decryption information is encrypted using the currently valid decryption information and may also include future decryption information and synchronization information.